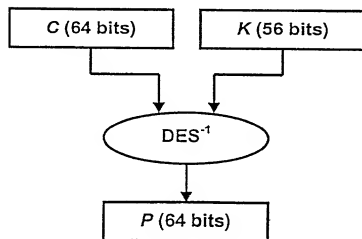
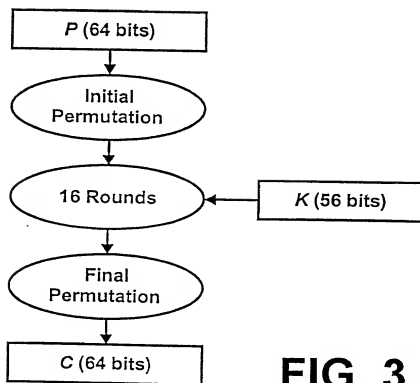


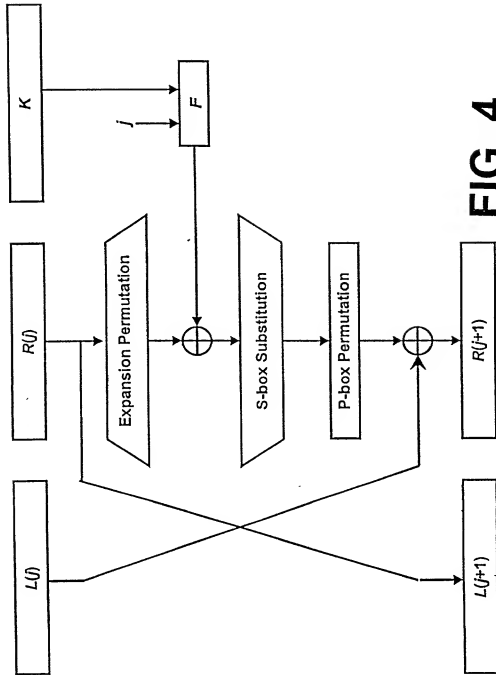
**FIG. 1**  
(Prior Art)



**FIG. 2**  
(Prior Art)



**FIG. 3**  
(Prior Art)



**FIG. 4**  
(Prior Art)

$y_1$	$y_2$	$y_3$	$y_4$	$y_5$	$y_6$	$y_7$	$y_8$	$y_9$	$y_{10}$	$y_{11}$	$y_{12}$
-------	-------	-------	-------	-------	-------	-------	-------	-------	----------	----------	----------



$k_1$	$k_2$	$k_3$	$k_4$	$k_5$	$k_6$	$k_7$	$k_8$	$k_9$	$k_{10}$	$k_{11}$	$k_{12}$
-------	-------	-------	-------	-------	-------	-------	-------	-------	----------	----------	----------

**FIG. 5**

$y_{13}$	$y_{14}$	$y_{15}$	$y_{16}$	$y_{17}$	$y_{18}$	$y_{19}$	$y_{20}$	$y_{21}$	$y_{22}$	$y_{23}$	$y_{24}$
----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------



$k_{13}$	$k_{14}$	$k_{15}$	$k_{16}$	$k_{17}$	$k_{18}$	$k_{19}$	$k_{20}$	$k_{21}$	$k_{22}$	$k_{23}$	$k_{24}$
----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------

**FIG. 6**

$y_{25}$	$y_{26}$	$y_{27}$	$y_{28}$	$y_{29}$	$y_{30}$	$y_{31}$	$y_{32}$	$y_{33}$	$y_{34}$	$y_{35}$	$y_{36}$
----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------



$k_{25}$	$k_{26}$	$k_{27}$	$k_{28}$	$k_{29}$	$k_{30}$	$k_{31}$	$k_{32}$	$k_{33}$	$k_{34}$	$k_{35}$	$k_{36}$
----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------

**FIG. 7**

$y_{37}$	$y_{38}$	$y_{39}$	$y_{40}$	$y_{41}$	$y_{42}$	$y_{43}$	$y_{44}$	$y_{45}$	$y_{46}$	$y_{47}$	$y_{48}$
----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------



$k_{37}$	$k_{38}$	$k_{39}$	$k_{40}$	$k_{41}$	$k_{42}$	$k_{43}$	$k_{44}$	$k_{45}$	$k_{46}$	$k_{47}$	$k_{48}$
----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------

**FIG. 8**

$x_{32}$	$x_1$	$x_2$	$x_3$	$x_4$	$x_5$	$x_6$	$x_7$	$x_8$	$x_9$	0	0
----------	-------	-------	-------	-------	-------	-------	-------	-------	-------	---	---

$\oplus$

FIG. 9

$k_1$	$k_2$	$k_3$	$k_4$	$k_5$	$k_6$	$k_9$	$k_{10}$	$k_{11}$	$k_{12}$	$(k_7 \oplus k_5)$	$(k_8 \oplus k_6)$
-------	-------	-------	-------	-------	-------	-------	----------	----------	----------	--------------------	--------------------

$x_8$	$x_9$	$x_{10}$	$x_{11}$	$x_{12}$	$x_{13}$	$x_{14}$	$x_{15}$	$x_{16}$	$x_{17}$	0	0
-------	-------	----------	----------	----------	----------	----------	----------	----------	----------	---	---

$\oplus$

FIG. 10

$k_{13}$	$k_{14}$	$k_{15}$	$k_{16}$	$k_{17}$	$k_{18}$	$k_{21}$	$k_{22}$	$k_{23}$	$k_{24}$	$(k_{19} \oplus k_{17})$	$(k_{20} \oplus k_{18})$
----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	--------------------------	--------------------------

$x_{16}$	$x_{17}$	$x_{18}$	$x_{19}$	$x_{20}$	$x_{21}$	$x_{22}$	$x_{23}$	$x_{24}$	$x_{25}$	0	0
----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	---	---



$k_{25}$	$k_{26}$	$k_{27}$	$k_{28}$	$k_{29}$	$k_{30}$	$k_{33}$	$k_{34}$	$k_{35}$	$k_{36}$	$(k_{31} \oplus k_{29})$	$(k_{32} \oplus k_{30})$
----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	--------------------------	--------------------------

FIG. 11

$x_{24}$	$x_{25}$	$x_{26}$	$x_{27}$	$x_{28}$	$x_{29}$	$x_{30}$	$x_{31}$	$x_{32}$	$x_1$	0	0
----------	----------	----------	----------	----------	----------	----------	----------	----------	-------	---	---



$k_{37}$	$k_{38}$	$k_{39}$	$k_{40}$	$k_{41}$	$k_{42}$	$k_{45}$	$k_{46}$	$k_{47}$	$k_{48}$	$(k_{43} \oplus k_{41})$	$(k_{44} \oplus k_{42})$
----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	--------------------------	--------------------------

FIG. 12